UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/514,119 | 02/28/2000 | Phyllis A Schneck | 62004-1330 | 9265 |

7590 04/05/2004

Tomas Kayden
Horstemeyer & Risley LLP
100 Georgia Parkway Suite 1750
Atlanta, GA 30339-5948

| EXAMINER | |
|---|---|
| ABRISHAMKAR, KAVEH | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | 7 |

DATE MAILED: 04/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) |
|---|---|---|
| | 09/514,119 | SCHNECK ET AL. |
| | Examiner | Art Unit |
| | Kaveh Abrishamkar | 2131 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on *09 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

## DETAILED ACTION

1. This office action is in response to the response filed on January 9, 2004, Paper No. 5. Original application contained claims 1-31. Applicant filed a terminal disclaimer for claims 1-3, 11-12, 17-20, 25-27, and 31. The terminal disclaimer filed on January 9, 2004 has been entered and made of record. Presently pending claims are 1-31.

### *Double Patenting*

2. Examiner acknowledges the terminal disclaimer, fully compliant with 37 CFR 3.73(b) filed by applicants on January 9, 2004. Accordingly, the double patenting rejection for claims 1-3, 11-12, 17-20, 25-27, and 31 has been overcome by virtue of the terminal disclaimer.

### *Response to Arguments*

3. Applicant's arguments filed on January 9, 2004, Paper. No. 5, have been fully considered but they are not persuasive for the following reasons:

The applicants in regards to claims 1-31 argue that the cited prior art [Kuroda U.S. Patent 5,935,248] does not teach "determining an actual security level in the receive host based upon the availability of a number of security processor operations." This argument is not found persuasive. Determination of an actual security level in the

receive host is recognized by the security level recognizing unit 11. The security level recognizing unit delineated by Kuroda by the nature of its function has to have some criteria for determining the security level in the receive host. The second part of the claim limitation states "based upon the availability of a number of security processor operations." Kuroda delineates the combination of multiple security operations to increase a resultant security level where encryption and authentication are cited as two processor operations that, when combined, increase the resultant security level (column 2 lines 1 – 25). Kuroda delineates the process of determining the security level in host depending on the "availability of a number of security processor operations." Kuroda describes the security-level recognizing unit which may recognize a security level from a receive host based on different security levels which depend on the availability of user authentication and/or encryption (column 7 line 24- column 8 line 65) which are described as security processor operations (column 2 lines 1 –25). Therefore, Kuroda does teach "determining an actual security level in the receive host based upon the availability of a number of security processor operations."

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the subject matter "determining an actual security level in the receive host based upon the availability of a number of security processor operations" broadly recited in the independent claims 1,11,18, and 25. The dependent claims 2-10,12-16,19-24, and 26-31 are rejected at least by virtue of their dependency on the independent claims and by other reason set forth in the previous office action (Paper No. 4). Accordingly, the rejections for claims 4-10, 13-16, 21-24, and 28-30 are

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuroda (U.S. 5,935,248).

Regarding claim 1, Kuroda discloses:

A method for applying adaptive security to a data stream, comprising the steps of:

identifying a desired security level range and a desired actual security level which falls within the desired security level range for communicating a data stream from a send host to a receive host (Figure 2 item 11, column 3 lines 62-67, column 4 lines 3-18);

determining an actual security level in the receive host based upon the availability of a number of security processor operations (column 3 lines 62-67, column 4 lines 3-18);

communicating the actual security level from the receive host to the send host (column 3 lines 62-67, column 4 lines 3-18, column 8 lines 40-46);

generating a plurality of data packets associated with the data stream in the send host, the data packets having an authentication header including the desired security level range and the actual security level (column 8 lines 40-46);

reallocating computing resources at the receive host if data packets cannot be verified at the desired actual security level with a current allocation of resources (column 7 lines 1-23); and

verifying the data packets at the actual security level, the actual security level being within the desired security level range (Figure 2 item 13, column 7 lines 48-54).

Regarding claim 2, Kuroda discloses:

The method of claim 1, further comprising the step of altering the actual security level in the send host using a security thermostat. (Figure 1 item 14, column 62-65).

Regarding claim 3, Kuroda discloses:

The method of claim 1, wherein the step of reallocating computing resources at the receive host comprises identifying the availability of a number of security operations per second (SOPS) employed in non-critical operations at the receive host and reallocating these SOPS for processing the data stream (column 6 lines 7-28).

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kuroda (U.S. 5,935,248) in view of Jurkevich et al. (U.S. 5,164,938).

Regarding claim 11, Kuroda discloses:

A method for communicating and applying adaptive security to a data stream comprising a plurality of data packets, comprising the steps of:

identifying a desired level range and a desired actual security level which falls within the desired security level range for the data stream to be received by a host (Figure 2 item 11, column 3 lines 62-67, column 4 lines 3-18);

determining the availability of a number of security processor operations at the host (column 3 lines 62-67, column 4 lines 3-18);

reallocating computing resources at the host if the data stream cannot be verified at the desired security level (column 7 lines 1-23);

verifying the data packets at the actual security level, the actual security level being within the desired security level range (Figure 2 item 13, column 7 lines 48-54).

Kuroda does not explicitly describe a method of reallocating communication resources if there are insufficient computing resources available for reallocation at the host.

Jurkevich teaches a method of:

reallocating communication resources if there are insufficient computing resources available for reallocation at the host (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to control the communication resources, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating communication resources between the different clients and servers, allowing for more efficient use of computing and communication resources.

Regarding claim 18, Kuroda discloses:

A system for facilitating data communication to a host with adaptive security comprising:

a means for determining whether a desired actual security level for a transmitted data stream falls within a desired security level range (Figure 2 item 11, column 3 lines 62-67, column 4 lines 3-18);

a means for determining the availability of a number of security processor operations at the host (column 3 lines 62-67, column 4 lines 3-18);

a means for reallocating computing resources at the host if the data stream cannot be verified at the desired security level (column 7 lines 1-23).

Kuroda does not explicitly describe a means of reallocating communication resources if there are insufficient computing resources available for reallocation at the host. Jurkevich teaches a method of a means for reallocating communication resources if there are insufficient computing resources available for reallocation at the host (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to control the communication resources, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating communication resources between the different

clients and servers, allowing for more efficient use of computing and communication resources.

Regarding claim 25, Kuroda discloses:

A computer program embodied on a computer-readable medium for facilitating data communication to a host with adaptive security, comprising:

logic configured to determine whether a desired actual security level for a transmitted data stream falls within a desired security level range (Figure 2 item 11, column 3 lines 62-67, column 4 lines 3-18);

logic configured to determine the availability of a number of security processor operations at the host (column 3 lines 62-67, column 4 lines 3-18);

logic configured to reallocate computing resources at the host if the data stream cannot be verified at the desired security level (column 7 lines 1-23).

Kuroda does not explicitly describe logic to reallocate communication resources if there are insufficient computing resources available for reallocation at the host. Jurkevich teaches a method of:

logic configured to reallocate communication resources if there are insufficient computing resources available for reallocation at the host (column 7 lines 27-32).

Jurkevich does not state that this reallocation of communication resources is to be used in an adaptive security method to be applied to a data stream. Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication

control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to control the communication resources, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating communication resources between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 4 is rejected applied above in rejecting claim 1. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of determining the bandwidth of the data stream being sent from the send host to the receive host. Jurkevich teaches determining the bandwidth of the data stream (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the

time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to recognize the bandwidth being used, through the use of Kuroda's communication control unit (Fig. 6 item 31), to recognize if communications resources are scarce. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 12 is rejected applied above in rejecting claim 11. Furthermore, Kuroda discloses:

The method of claim 11, wherein the step of reallocating computing resources at the host comprises identifying the availability of a number of security operations per second (SOPS) employed in non-critical operations at the host and reallocating these SOPS for processing the data stream (column 6 lines 7-28).

Claim 13 is rejected applied above in rejecting claim 11. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth of the data stream. Jurkevich teaches the step of reallocating

communication resources comprising adjusting the bandwidth of a data stream (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 17 is rejected applied above in rejecting claim 11. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly mention the step of using communication resources to calibrate the computing resources. Jurkevich teaches the step of calibrating the computing resources with the communication resources (column 31 lines 14-28).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6,

column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to calibrate the computing resources using the communication resources through the use of Kuroda's communication control unit (Fig. 6 item 31). This system would allow hosts with insufficient computing resources to handle a certain number of security operations to be calibrated with the available communication resources so that to increase the ability of multiple hosts to handle more security operations per second.

Claim 19 is rejected applied above in rejecting claim 18. Furthermore, Kuroda discloses:

The system of claim 18, wherein the means for determining the availability of a number of security processor operations comprises means for determining a processor time availability by examining a resource tracking table for non-critical processor time usage of at least one existing data stream (column 3 lines 62-67, column 4 lines 3-18).

Claim 20 is rejected applied above in rejecting claim 18. Furthermore, Kuroda discloses:

The system of claim 18, wherein the means for determining the availability of a number of security processor operations comprises means for identifying the availability

of a number of security processor per second (SOPS) employed in non-critical operations at the host and reallocating these SOPS for processing the data stream (column 7 lines 1-23).

Claim 21 is rejected applied above in rejecting claim 18. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth of the data stream. Jurkevich teaches the step of reallocating communication resources comprising adjusting the bandwidth of a data stream (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility

in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 24 is rejected applied above in rejecting claim 18. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly mention the step of using communication resources to calibrate the computing resources. Jurkevich teaches the step of calibrating the computing resources with the communication resources (column 31 lines 14-28). Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to calibrate the computing resources using the communication resources through the use of Kuroda's communication control unit (Fig. 6 item 31). This system would allow hosts with insufficient computing resources to handle a certain number of security operations to be calibrated with the available communication resources so that to increase the ability of multiple hosts to handle more security operations per second.

Claim 26 is rejected applied above in rejecting claim 25. Furthermore, Kuroda discloses:

The computer program of claim 25, wherein the logic configured to determine the availability of a number of security processor operations comprises logic configured to determine a processor time availability by examining a resource tracking table for a non-critical processor time usage of at least one existing data stream (column 3 lines 62-67, column 4 lines 3-18).

Claim 27 is rejected applied above in rejecting claim 25. Furthermore, Kuroda discloses:

The computer program of claim 25, wherein the logic configured to determine the availability of a number of security processor operations comprises logic configured to identify the availability of a number of security operations per second (SOPS) employed in non-critical operations at the host and reallocate these SOPS available for processing the data stream (column 7 lines 1-23).

Claim 28 is rejected applied above in rejecting claim 25. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the logic of reallocating communication resources by adjusting the bandwidth of the data stream. Jurkevich teaches the step of reallocating

communication resources comprising adjusting the bandwidth of a data stream (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 31 is rejected applied above in rejecting claim 25. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly mention the step of using communication resources to calibrate the computing resources. Jurkevich teaches the step of calibrating the computing resources with the communication resources (column 31 lines 14-28).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6,

column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to calibrate the computing resources using the communication resources through the use of Kuroda's communication control unit (Fig. 6 item 31). This system would allow hosts with insufficient computing resources to handle a certain number of security operations to be calibrated with the available communication resources so that to increase the ability of multiple hosts to handle more security operations per second.

Claim 5 is rejected applied above in rejecting claim 4. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. Kuroda does not explicitly describe a method of reallocating communication resources if there are insufficient computing resources available for reallocation at the host. Jurkevich teaches a method of:

reallocating communication resources if there are insufficient computing resources available for reallocation at the host (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to control the communication resources, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating communication resources between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 14 is rejected applied above in rejecting claim 13. Furthermore, Kuroda discloses the step of identifying the number of security operations per second (SOPS) that will be required to process the data stream and comparing this number with the number of SOPS available at the receive host. However, Kuroda does not explicitly note that the determination of the number of security operations at the host would determine the amount of bandwidth adjustment needed. Jurkevich teaches that bandwidth management can be based on a number of factors attributed to priority including loss tolerance, average packet length, and activity level (column 21 lines 10-35). This activity level can be interpreted as the number of security operations at the receive host.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kuroda and Jurkevich to gain the flexibility of not only reallocating the computing resources when there is insufficient computing power at a host, but to also reallocate the bandwidth to obtain the maximum use of the available resources.

Claim 15 is rejected applied above in rejecting claim 13. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth by decreasing the transmission rate. Jurkevich teaches a method, wherein the bandwidth is adjusted by decreasing the transmission rate (column 28 lines 50-63).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by decreasing the transmission rate, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources

at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 16 is rejected applied above in rejecting claim 13. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of the data packets. Jurkevich teaches a method of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of data packets(column 3 lines 18-22, column 20 lines 54-61, column 26 lines 51-53). Kuroda does not explicitly state that the bandwidth is adjusted by increasing the security:message ratio of the data packets, however, Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by increasing the security:message ratio of the data packets. This would

beneficial if the multiple server to client connections needed more bandwidth for the security operations. The increase in security:message ratio of the data packets would increase the bandwidth available to support the security operations.

Claim 22 is rejected applied above in rejecting claim 21. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth by decreasing the transmission rate. Jurkevich teaches a method, wherein the bandwidth is adjusted by decreasing the transmission rate (column 28 lines 50-63).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by decreasing the transmission rate, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the

different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 23 is rejected applied above in rejecting claim 21. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of the data packets. Jurkevich teaches a method of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of data packets(column 3 lines 18-22, column 20 lines 54-61, column 26 lines 51-53). Kuroda does not explicitly state that the bandwidth is adjusted by increasing the security:message ratio of the data packets, however, Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by increasing the security:message ratio of the data packets. This would beneficial if the multiple server to client connections needed more bandwidth for the

security operations. The increase in security:message ratio of the data packets would increase the bandwidth available to support the security operations.

Claim 29 is rejected applied above in rejecting claim 28. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the logic of reallocating communication resources by adjusting the bandwidth by decreasing the transmission rate. Jurkevich teaches a method, wherein the bandwidth is adjusted by decreasing the transmission rate (column 28 lines 50-63).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by decreasing the transmission rate, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the

different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 30 is rejected applied above in rejecting claim 28. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the logic of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of the data packets. Jurkevich teaches a method of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of data packets(column 3 lines 18-22, column 20 lines 54-61, column 26 lines 51-53). Kuroda does not explicitly state that the bandwidth is adjusted by increasing the security:message ratio of the data packets, however, Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by increasing the security:message ratio of the data packets. This would beneficial if the multiple server to client connections needed more bandwidth for the

security operations. The increase in security:message ratio of the data packets would increase the bandwidth available to support the security operations.

Claim 6 is rejected applied above in rejecting claim 5. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth of the data stream. Jurkevich teaches the step of reallocating communication resources comprising adjusting the bandwidth of a data stream (column 7 lines 27-32).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 7 is rejected applied above in rejecting claim 6. Furthermore, Kuroda discloses the step of identifying the number of security operations per second (SOPS) that will be required to process the data stream and comparing this number with the number of SOPS available at the receive host. However, Kuroda does not explicitly note that the determination of the number of security operations at the host would determine the amount of bandwidth adjustment needed. Jurkevich teaches that bandwidth management can be based on a number of factors attributed to priority including loss tolerance, average packet length, and activity level (column 21 lines 10-35). This activity level can be interpreted as the number of security operations at the receive host. Therefore it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kuroda and Jurkevich to gain the flexibility of not only reallocating the computing resources when there is insufficient computing power at a host, but to also reallocate the bandwidth to obtain the maximum use of the available resources.

Claim 8 is rejected applied above in rejecting claim 6. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of reallocating communication resources by adjusting the bandwidth by decreasing the transmission rate. Jurkevich teaches a

method, wherein the bandwidth is adjusted by decreasing the transmission rate (column 28 lines 50-63).

Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by decreasing the transmission rate, through the use of Kuroda's communication control unit (Fig. 6 item 31), if there are insufficient computing resources at one of the clients. This system developed from the combination of the teachings of Jurkevich and Kuroda allows for more flexibility in allocating bandwidth between the different clients and servers, allowing for more efficient use of computing and communication resources.

Claim 9 is rejected applied above in rejecting claim 6. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly describe the step of adjusting bandwidth by increasing a data portion of the data packets to lower a security:message ratio of the data packets. Jurkevich teaches a method of adjusting bandwidth by increasing a data portion of the

data packets to lower a security:message ratio of data packets(column 3 lines 18-22, column 20 lines 54-61, column 26 lines 51-53). Kuroda does not explicitly state that the bandwidth is adjusted by increasing the security:message ratio of the data packets, however, Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6, column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to adjust the bandwidth by increasing the security:message ratio of the data packets. This would beneficial if the multiple server to client connections needed more bandwidth for the security operations. The increase in security:message ratio of the data packets would increase the bandwidth available to support the security operations.

Claim 10 is rejected applied above in rejecting claim 6. Furthermore, Kuroda discloses a method of communicating and applying adaptive security to a data stream. Kuroda further teaches identifying a desired security level, determining the availability of security operations at the host, and reallocating computing resources. However, Kuroda does not explicitly mention the step of using communication resources to calibrate the computing resources. Jurkevich teaches the step of calibrating the computing resources with the communication resources (column 31 lines 14-28). Kuroda delineates a scenario with a plurality of server and client apparatuses (Figure 6,

column 8 lines 34-45) comprising of different data streams. Also, Kuroda describes a communication control unit (Figure 6, item 31) that controls communications between servers and clients. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Kuroda and Jurkevich, to achieve an adaptive security method that also has the ability to calibrate the computing resources using the communication resources through the use of Kuroda's communication control unit (Fig. 6 item 31). This system would allow hosts with insufficient computing resources to handle a certain number of security operations to be calibrated with the available communication resources so that to increase the ability of multiple hosts to handle more security operations per second.

## *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
03/23/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100